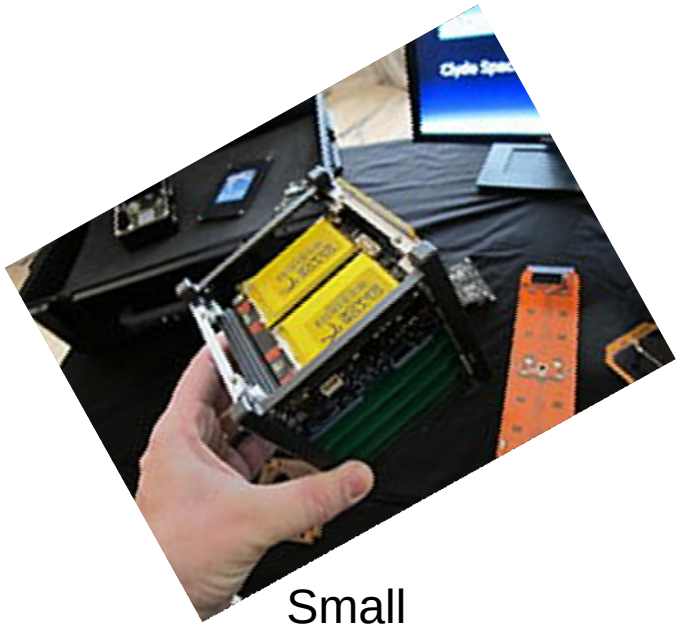
Spaceflight Reliability: An Objectives-Based Strategy

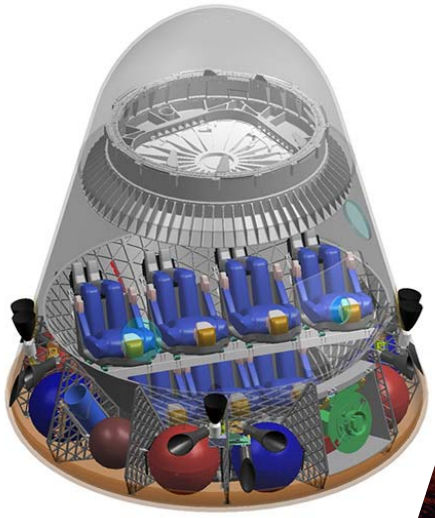
John Evans, Frank Groen – NASA OSMA

TRISMAC 2015
ESRIN, Frascati, Italy

NASA Challenges

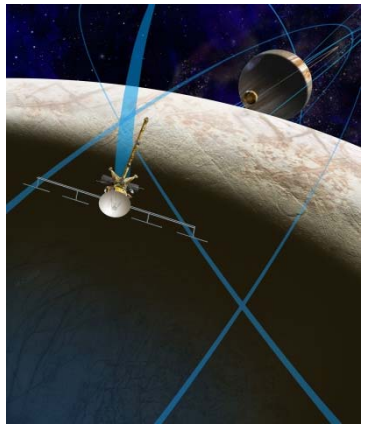


Small Sats



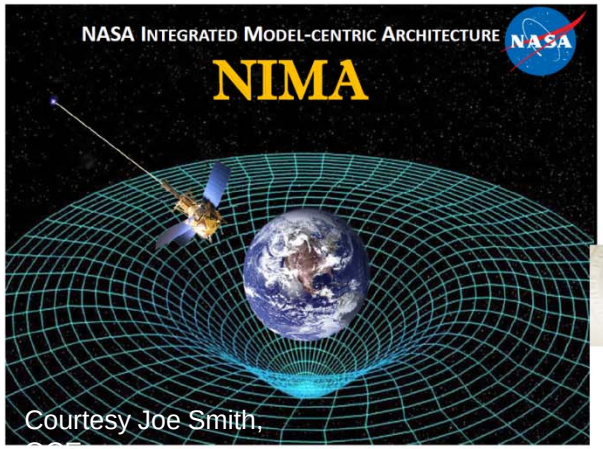
Commercial Crew

Mars



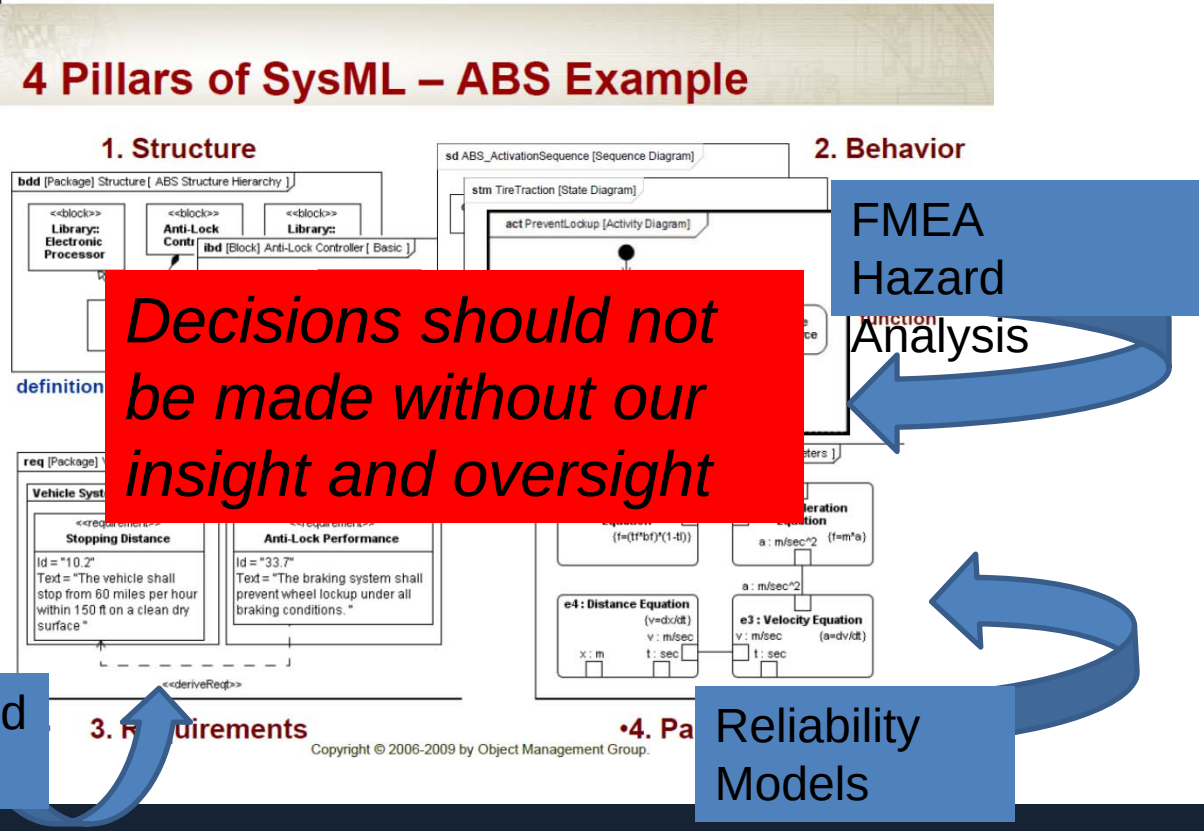
Europa and Beyond

MBSE



Our products may need to be different in a model based environment

NASA OCE direction *will* enable model centric capability



Decisions should not be made without our insight and oversight

FMEA Hazard Analysis

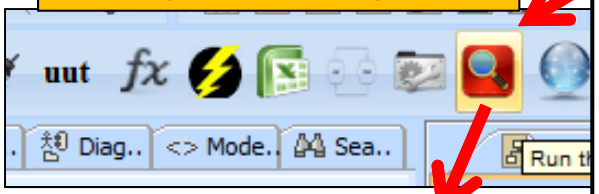
Safety Requirements and Quality Demands

Reliability Models

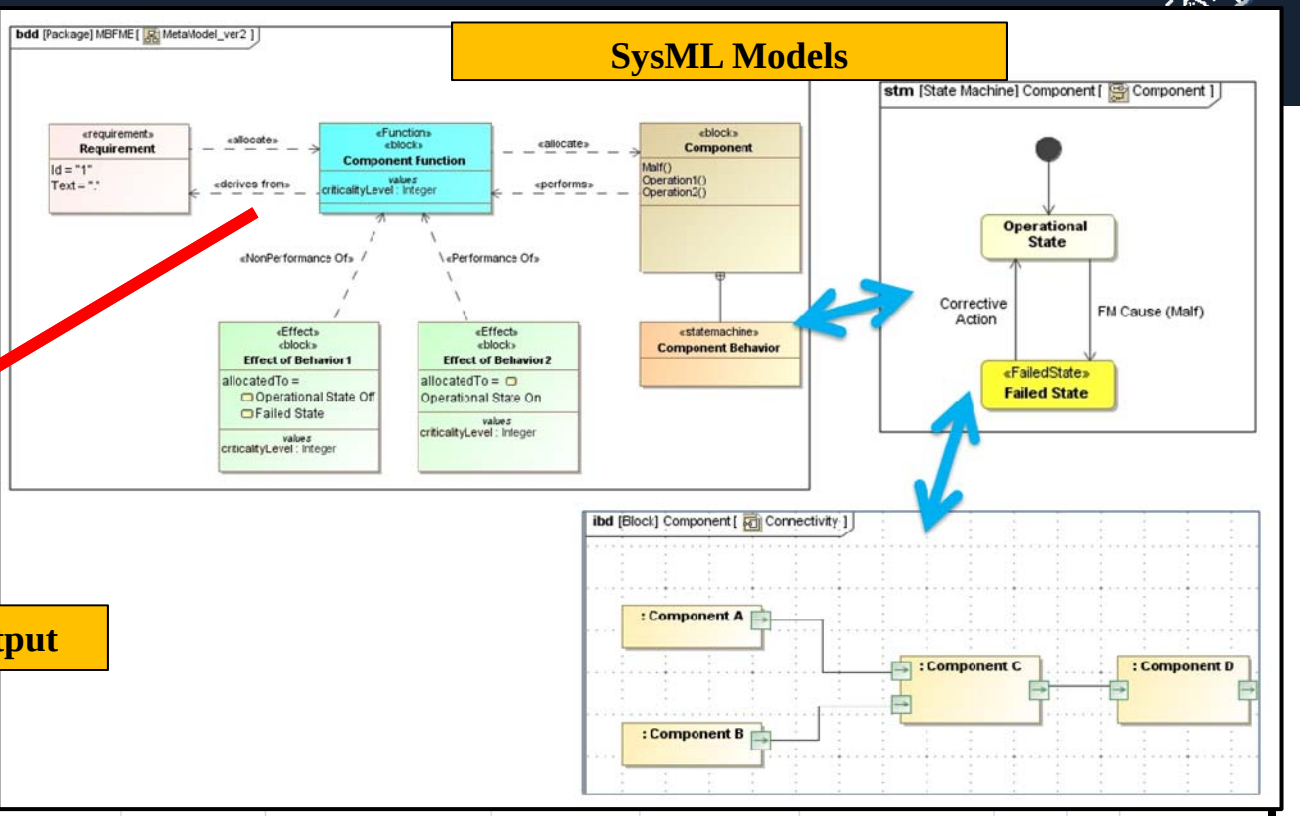
MBSE FMEA

Courtesy Lui Wang
Johnson Space Center

Magic Draw Plug-Ins



SysML Models



FMECA Output

Failure Modes and Effects Criticality Ana

Project Name:	Fan in the Can SysML Model

System	Subsystem	LRU/ Assembly Type	LRU/ Assembly Name	Item Function	Potential Failure Mode	Effect				CRIT LEVEL	SEV	Potential Causes
						Immediate Failure Effect	End Effect	Number of Independent	Other Independent Failures			
FaninCan	ECLSS	CCAA	CCAA1	CCAA1 Ciruculates Air	Failed Off	Loss of CCAA1 air Circultation	Loss of CCAA1 air Circultation	1		1		Internal Malf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed Off	Loss_of_Mbsu1_output_power	Loss of CCAA1 air Circultation	2	MBSU2 Failed Off	1		insertInternalMalf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed On	MBSU1_Ouput_Power_On						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed On	Loss_of_ability_to_manage_MBSU1_loads						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed Off	Loss_of_Mbsu2_output_power	Loss of CCAA1 air Circultation	2	MBSU1 Failed Off	1		insertInternalMalf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed On	MBSU2_Ouput_Power_On						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed On	Loss_of_ability_to_manage_MBSU2_loads						insertInternal2Malf
FaninCan	Power Subsystem	PDU	PDU1	PDU_Distribute_Power	Failed Off	Loss_of_PDU_output_power	Loss of CCAA1 air Circultation	1		1		insertInternalMalf
FaninCan	Power Subsystem	PDU	PDU1	PDU_Distribute_Power	Failed On	PDU_Output_Power_On						insertInternal2Malf

Mission Assurance Challenges

- NASA's Mission Assurance faces challenges
  - Changing missions
  - Changing acquisition models
  - Changing engineering practices
  - Changing technology

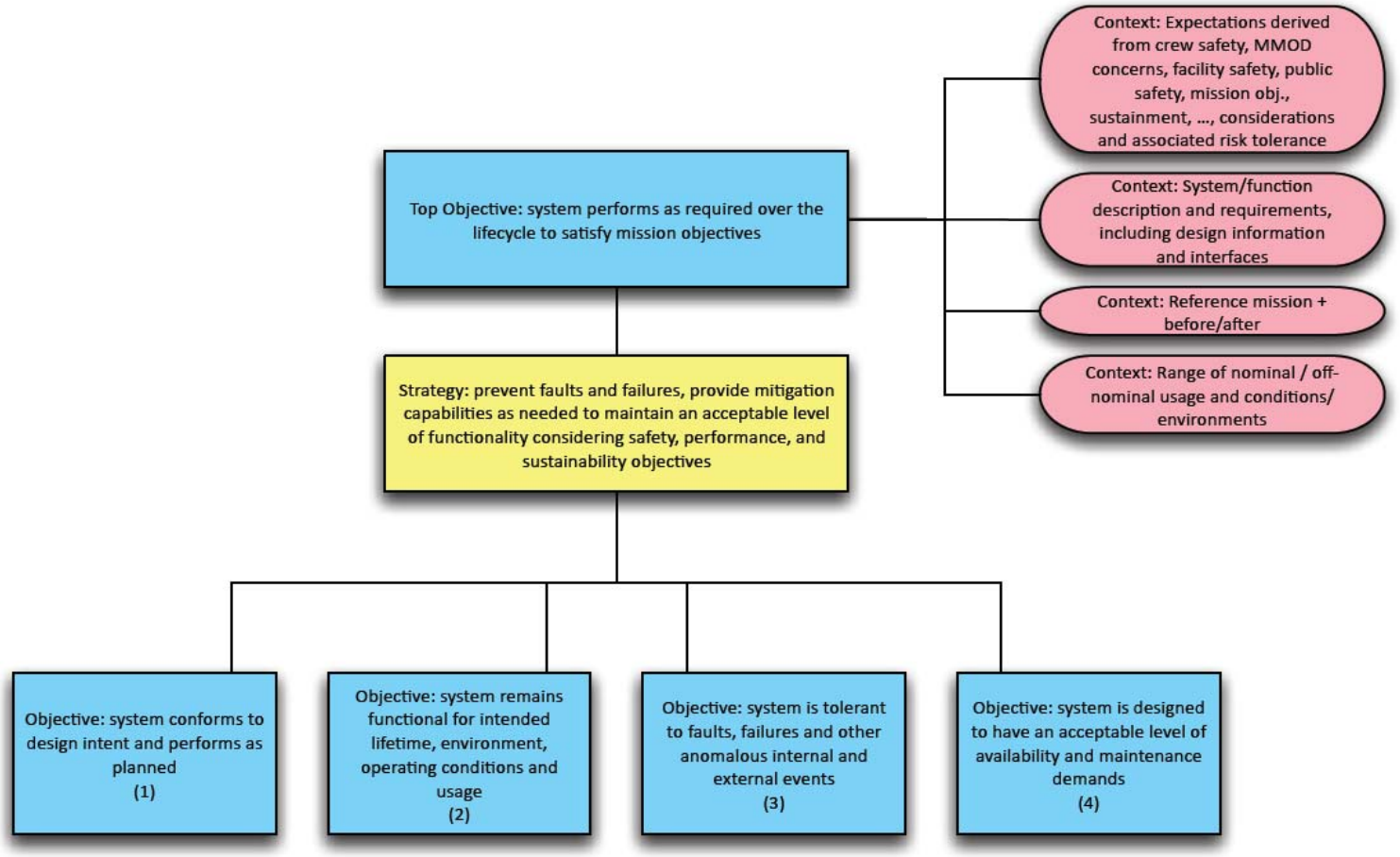
- We must reconsider our practices to stay relevant
  - Don't necessarily hang on to 'proven' practices
  - Consider the intent behind R&M methods and techniques

“Subset of Considerations”

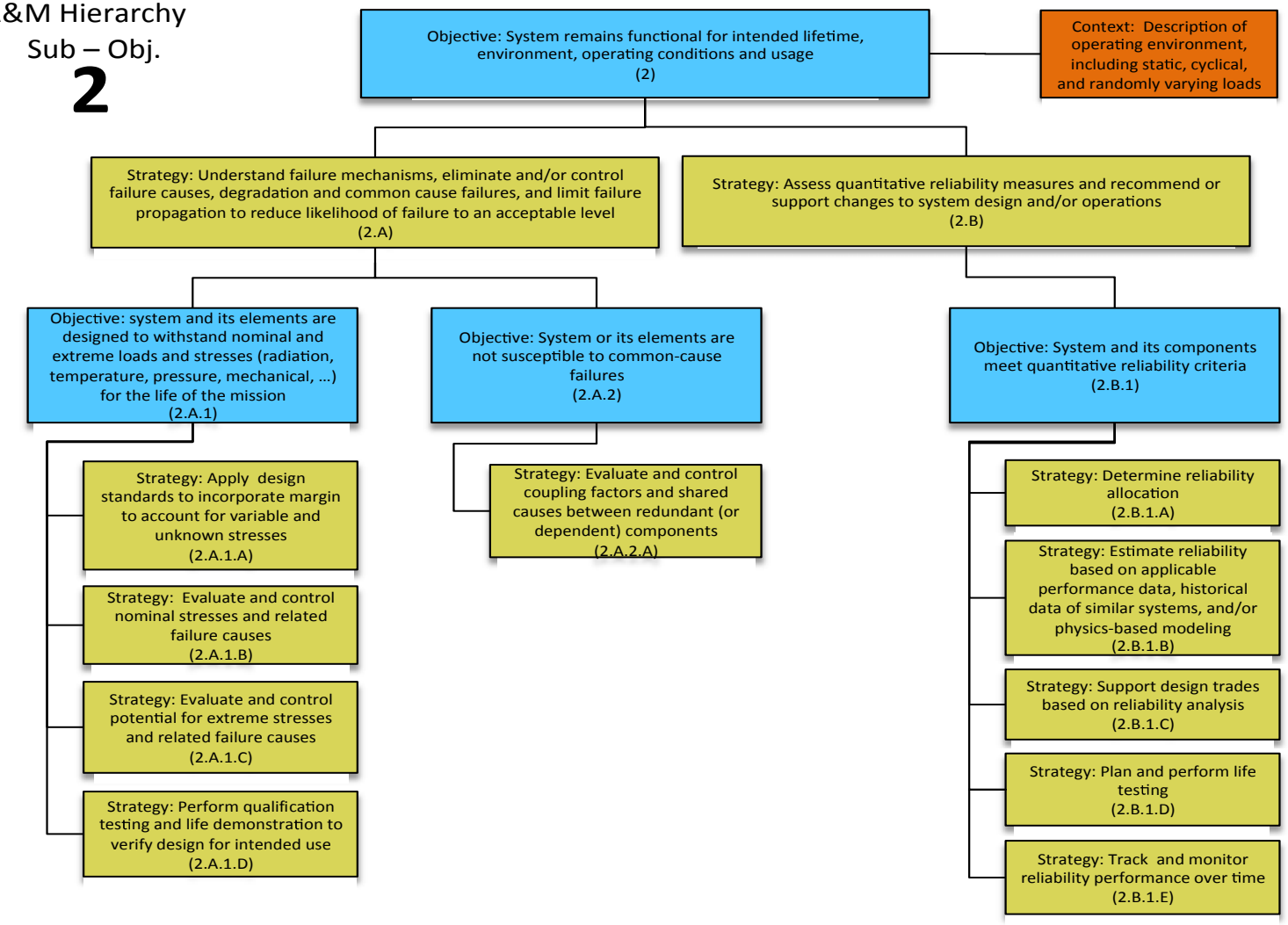
- Focus on the *what*:
  - Emphasize R&M objectives and related strategies
  - Provide greater flexibility to select methods and techniques
  - Allow for innovation and adaptation to new engineering practices
  - Facilitate self-assessment and independent review

Decomposition of R&M Objectives

R&M Objectives Structure – Top-Level



R&M Hierarchy
Sub – Obj.
2



Laying the Foundation

- Logically decompose top-level R&M objective
  - Use elements of the Goal Structuring Notation
  - Structure shows why strategies are to be applied

- Structure forms basis for a proposed R&M standard
  - Specifies the technical considerations to be addressed by projects
  - Forms basis for evaluation of plans, design, and assurance products

Summary

- Changes in missions, acquisition/engineering practices, and technology challenge proven R&M practices
- Define R&M objectives and strategies to enable adaptation and innovation
- Logically decompose the top-level R&M objective to identify the elements of an R&M argument